Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

podpůrný materiál 4.2-2

# Návod pro prioritizaci rizik správy dat

verze 1.0

vytvořeno v rámci projektu

*Zajištění podmínek pro kvalitní správu datového fondu a zajištění řízeného přístupu k datům*

*Reg.č.: CZ.31.1.01/MV/23_62/000006*

# Obsah

# 1 Účel a vazba návodu na metodiku řízení rizik správy dat

Dokument navazuje na „Metodiku řízení rizik správy dat“ a doplňuje ji v části prioritizace. Metodika stanoví principy, návod poskytuje referenční a doporučený přístup k prioritizaci rizik správy dat, hodnotící škály a výpočet priority. Organizace mohou použít i jiný způsob prioritizace, pokud je tento způsob v souladu s principy stanovenými „Metodikou řízení rizik správy dat“, zejména pokud vychází z posouzení dopadů rizik správy dat, reflektuje význam dat pro agendy a rozhodování organizace a umožňuje transparentní a obhajitelné určení priority rizik.

Bez ohledu na zvolený postup by výsledky prioritizace rizik správy dat měly být srovnatelné svým významem a využitelností. To znamená, že organizace by měla být schopna rozlišit rizika s nízkou, střední, vysokou a kritickou prioritou, vysvětlit důvody tohoto zařazení a použít výstupy prioritizace jako podklad pro řízení opatření, plánování kapacit a rozhodování vedení.

Výsledky prioritizace rizik správy dat mohou rovněž sloužit jako vstup do řízení rizik kybernetické bezpečnosti v případech, kdy rizika správy dat dosahují významných dopadů na regulované služby nebo klíčová aktiva organizace.

# 2 Základní principy prioritizace rizik správy dat

Prioritizace rizik správy dat slouží k určení relativního významu jednotlivých rizik a k podpoře rozhodování o tom, kterým rizikům je vhodné věnovat pozornost přednostně. Nejde o snahu přesně kvantifikovat rizika ani o vytvoření úplného pořadí všech identifikovaných rizik, ale o vytvoření praktického a srozumitelného základu pro další práci s riziky.

Prioritizace rizik správy dat vychází z principů stanovených v „Metodice řízení rizik správy dat“ a je úzce provázána s významem dat pro fungování organizace, plnění jejích agend a podporu rozhodování. Tyto principy tvoří rámec, ve kterém se pohybuje i tento návod.

## 2.1 Prioritizace založená na dopadu

Základním principem prioritizace rizik správy dat je posuzování rizik podle jejich dopadu, nikoli podle pravděpodobnosti jejich výskytu. Tento přístup reflektuje skutečnost, že i rizika s nízkou pravděpodobností mohou mít v případě realizace zásadní následky pro organizaci, zejména pokud se týkají významných dat nebo klíčových agend.

Dopad rizika správy dat vyjadřuje závažnost následků, které by realizace rizika měla na fungování organizace, kvalitu rozhodování nebo plnění zákonných a strategických úkolů. Hodnocení dopadu je proto klíčovým vstupem pro stanovení priority rizika.

## 2.2 Relativní a kontextový charakter priority

Priorita rizika správy dat nemá absolutní význam a vždy závisí na kontextu konkrétní organizace. Stejné riziko správy dat může mít v různých organizacích odlišnou prioritu v závislosti na:

- významu dotčených dat,
- způsobu jejich využití,
- existujících opatřeních a schopnosti organizace riziko zvládat.

Prioritizace proto neslouží k porovnávání rizik mezi organizacemi, ale k internímu rozhodování v rámci jedné organizace. Výsledkem prioritizace by mělo být rozlišení rizik podle jejich významu tak, aby bylo zřejmé, kterým rizikům se má organizace věnovat přednostně.

## 2.3 Vazba prioritizace na další řízení rizik

Stanovení priority rizika správy dat je prostředkem, nikoli cílem. Priorita rizika slouží zejména jako vstup pro:

- plánování a řízení opatření v oblasti správy dat,
- alokaci kapacit a zdrojů,
- komunikaci rizik směrem k vedení organizace.

V případech, kdy rizika správy dat dosahují významných dopadů na regulované služby nebo klíčová aktiva, mohou výsledky prioritizace sloužit také jako podklad pro návaznost na řízení rizik kybernetické bezpečnosti.

## 2.4 Oddělení prioritizace a návrhu opatření

Prioritizace rizik správy dat neznamená automaticky rozhodnutí o konkrétních opatřeních. Stanovení priority odpovídá na otázku, která rizika jsou významná, nikoli na otázku, *jakým způsobem mají být řešena*. Návrh, realizace a vyhodnocování opatření jsou samostatnými kroky, které navazují na prioritizaci, ale nejsou její součástí.

Toto oddělení podporuje přehlednost řízení rizik a zabraňuje tomu, aby byla priorita rizika ovlivňována dostupností nebo náročností opatření.

# 3 Vstupy do hodnocení dopadu a prioritizace rizik správy dat

Hodnocení dopadu a stanovení priority rizik správy dat předpokládá, že organizace má k dispozici základní vstupní informace, které umožňují posoudit význam rizika v konkrétním kontextu.

## 3.1 Identifikované riziko správy dat

Základním vstupem je konkrétní identifikované riziko správy dat, které je předmětem hodnocení. Riziko by mělo být jednoznačně popsáno tak, aby bylo zřejmé:

- jaké situace nebo nedostatku ve správě dat se týká,
- v jaké části organizace nebo datové oblasti se projevuje,
- jaký je jeho vztah ke katalogu rizik správy dat.

Hodnocení dopadu se vždy vztahuje ke konkrétnímu riziku správy dat, nikoli k obecnému problému nebo oblasti správy dat jako celku.

## 3.2 Kontext rizika a vazba na organizaci

Pro posouzení dopadu je nezbytné znát organizační a věcný kontext, ve kterém se riziko správy dat uplatňuje. Zejména je vhodné mít k dispozici informace o:

- dotčených datových oblastech,
- vazbě rizika na konkrétní agendy, procesy nebo rozhodovací činnosti,
- významu těchto agend a procesů pro fungování organizace.

Tyto informace umožňují posoudit, zda se jedná o riziko okrajové, nebo o riziko s potenciálně významnými dopady.

## 3.3 Určení primárního a sekundárních dopadů

Před zahájením hodnocení dopadu je nutné určit, jaké dopady může realizace rizika správy dat mít. U každého rizika by měl být identifikován:

- jeden primární dopad, který nejlépe vystihuje hlavní význam rizika,
- případně jeden nebo více sekundárních dopadů, které popisují další relevantní následky.

Primární a sekundární dopady se určují s využitím typových dopadů katalogu rizik správy dat. Jasné vymezení primárního dopadu je klíčovým předpokladem pro následné hodnocení dopadu a stanovení priority rizika.

## 3.4 Informace o existujících opatřeních a stavu správy dat

Hodnocení dopadu by mělo zohledňovat také aktuální stav správy dat a existující opatření, která mohou ovlivňovat následky realizace rizika. Zejména se jedná o informace o:

- zavedených pravidlech, postupech nebo kontrolách,
- odpovědnostech v oblasti správy dat,
- technických nebo organizačních opatřeních, která mohou zmírnit dopady rizika.

Tyto informace neslouží k hodnocení pravděpodobnosti rizika, ale k realistickému posouzení jeho možných následků v daném prostředí.

## 3.5 Vazby na další oblasti řízení

Součástí vstupních informací mohou být také údaje o vazbách rizika správy dat na další oblasti řízení, zejména na:

- řízení změn informačních systémů,
- řízení kontinuity činností,
- řízení rizik kybernetické bezpečnosti.

Tyto vazby nejsou podmínkou pro samotné hodnocení dopadu, ale mohou poskytnout důležitý kontext pro interpretaci výsledků a pro rozhodování o dalších krocích, zejména v případech s významnými nebo kombinovanými dopady.

## 3.6 Poznámka k evidenci informací o rizicích správy dat

Tento návod nepředepisuje konkrétní způsob evidence informací o rizicích správy dat, včetně popisu dopadů, jejich hodnocení ani výsledné priority. Způsob zaznamenávání těchto informací závisí na potřebách, zvyklostech a úrovni zralosti konkrétní organizace a může vycházet z již používaných nástrojů nebo postupů v oblasti řízení rizik, správy dat nebo kybernetické bezpečnosti.

Důležité je, aby zvolený způsob evidence umožňoval zpětné dohledání hodnocení, jejich odůvodnění a návaznost na další kroky řízení rizik.

# 4 Hodnocení dopadu rizika správy dat

## 4.1 Účel hodnocení dopadu

Smyslem hodnocení dopadu není exaktní kvantifikace škody ani vytvoření matematického modelu rizika. Hodnocení dopadu představuje strukturovaný odborný odhad, který má být srozumitelný,

konzistentní a obhajitelný. Slouží jako praktický nástroj pro podporu rozhodování, nikoli jako samoúčelný analytický výstup.

## 4.2 Vztah hodnocení dopadu k typovým dopadům rizik správy dat

Rizika správy dat mohou mít více různých dopadů, které se mohou projevit současně nebo v různých rovinách fungování organizace. Pro účely jednotného a srovnatelného popisu dopadů využívá katalog rizik správy dat typové dopady (TD1–TD14), které představují standardizovaný soubor možných následků realizace rizik správy dat.

U každého rizika správy dat je nutné určit jeden primární dopad, který nejlépe vystihuje hlavní význam a podstatu rizika. Primární dopad vyjadřuje, *v čem spočívá nejzávažnější následek realizace daného rizika* z pohledu organizace, jejích agend a rozhodování. Vedle primárního dopadu mohou být u rizika identifikovány také sekundární dopady, které popisují další relevantní následky, jež však nejsou dominantní.

Pro účely hodnocení dopadu a stanovení priority rizika správy dat se hodnotí výhradně primární dopad rizika. Kritéria hodnocení dopadu uvedená v následující kapitole se vztahují k primárnímu dopadu a slouží k určení jeho závažnosti v konkrétním organizačním kontextu. Tento přístup podporuje srozumitelnost, konzistenci a obhajitelnost výsledků prioritizace.

Sekundární dopady se do samotného hodnocení dopadu nezapočítávají, nejsou váženy ani agregovány. Jejich identifikace má však důležitou podpůrnou roli a slouží zejména k:

- lepšímu pochopení širšího kontextu rizika,
- podpoře návrhu vhodných nápravných a preventivních opatření,
- posouzení, zda riziko správy dat může mít významné vazby na regulované služby nebo klíčová aktiva organizace.

V případech, kdy sekundární dopady naznačují možné významné dopady v oblasti kybernetické bezpečnosti, mohou sloužit jako jeden z podkladů pro rozhodnutí o eskalaci rizika správy dat do řízení rizik kybernetické bezpečnosti. Tato eskalace se však opírá o celkový kontext rizika a jeho dopadů a nemění skutečnost, že stanovení priority rizika správy dat vychází z hodnocení jeho primárního dopadu

## 4.3 Kritéria hodnocení dopadu

Pro účely tohoto návodu je hodnocení dopadu založeno na posouzení dopadu z několika vzájemně se doplňujících hledisek (kritérií). Tato kritéria představují doporučený referenční rámec, který organizacím pomáhá uvažovat o dopadech rizik správy dat systematicky a konzistentně. Organizace mohou kritéria upravit, rozšířit nebo zjednodušit, pokud tím není narušen soulad s principy uvedenými v „Metodice řízení rizik správy dat“.

Pro podporu posouzení dopadů mohou organizace využít hodnoticí otázky uvedené v samostatném dokumentu „Příloha - hodnoticí otázky dopadů“.

### K1 – Rozsah dopadu

Kritérium posuzuje, jak velké části organizace se dopad rizika týká. Zohledňuje zejména:

- rozsah dotčených datových oblastí,
- v případě rizik s plošným dopadem počet nebo význam dotčených agend a procesů,
- okruh interních nebo externích uživatelů, kteří jsou dopadem zasaženi.

Vyšší hodnota kritéria odpovídá situacím, kdy dopad rizika zasahuje více klíčových oblastí organizace nebo má plošný charakter.

### K2 – Závažnost dopadu na fungování a rozhodování

Kritérium posuzuje, jak závažné následky má realizace rizika na schopnost organizace fungovat a rozhodovat. Zohledňuje zejména:

- omezení nebo narušení plnění zákonných nebo strategických úkolů,
- snížení kvality nebo spolehlivosti rozhodování,
- vznik významných provozních problémů v důsledku nedostupnosti, nekvality nebo nesprávné interpretace dat.

Vyšší hodnota kritéria odpovídá situacím, kdy dopad rizika významně omezuje klíčové činnosti organizace nebo vede k zásadně chybným rozhodnutím.

### K3 – Náročnost nápravy a obnovy

Kritérium posuzuje, jak obtížné je odstranit následky realizovaného rizika a obnovit správný stav. Zohledňuje zejména:

- časovou náročnost nápravy,
- potřebu zapojení více útvarů nebo externích subjektů,
- finanční, personální nebo organizační náročnost obnovy.

Vyšší hodnota kritéria odpovídá situacím, kdy je náprava zdlouhavá, nákladná nebo organizačně složitá a kdy dopady přetrvávají delší dobu.

### K4 – Reputační, právní a strategické dopady

Kritérium posuzuje dopady, které přesahují bezprostřední provozní rovinu. Zohledňuje zejména:

- možné poškození důvěry veřejnosti, partnerů nebo dozorových orgánů,
- riziko právních důsledků, sankcí nebo sporů,
- negativní dopad na dlouhodobé strategické cíle organizace.

Vyšší hodnota kritéria odpovídá situacím, kdy realizace rizika může mít dlouhodobé nebo obtížně vratné následky mimo každodenní provoz organizace.

### Použití kritérií v praxi

Při hodnocení dopadu rizika správy dat se doporučuje posoudit všechna uvedená kritéria samostatně a výsledky zaznamenat (organizace si zvolí vlastní způsob práce s kritérii a zaznamenání výsledků).

Kritéria nejsou určena k mechanickému vyplňování ani k detailnímu kvantitativnímu modelování. Jejich hlavním účelem je podpořit strukturovanou odbornou diskusi a zajistit, aby byly při hodnocení dopadu systematicky zohledněny různé roviny dopadu rizik správy dat.

## 4.4 Doporučený postup stanovení úrovně dopadu

Jako referenční postup se doporučuje využít bodovou škálu, která umožňuje převést hodnocení jednotlivých kritérií na výslednou úroveň dopadu. Konkrétní podoba škály a způsob agregace mohou být přizpůsobeny potřebám organizace, následující postup představuje jednu z možných variant.

Organizace nejprve přiřadí jednotlivým kritériím hodnocení dopadu hodnoty na zvolené škále, a to s ohledem na význam primárního dopadu v konkrétním kontextu organizace.

> ***Příklad: každému kritériu se přiřadí hodnota na škále 1–5:***
>
> - *1 = zanedbatelný dopad,*
> - *5 = velmi závažný dopad.*

Následně se hodnoty jednotlivých kritérií agregují do výsledného vyjádření dopadu. Agregace může být provedena například:

- součtem hodnot jednotlivých kritérií,
- nebo jiným jednoduchým a transparentním způsobem, který organizace dlouhodobě používá.

Na základě agregovaného výsledku se stanoví výsledná úroveň dopadu (například nízká, střední, vysoká a kritická). Přesné vymezení hranic mezi jednotlivými úrovněmi dopadu není tímto návodem předepsáno a může se lišit v závislosti na velikosti, působnosti a zralosti organizace.

**Příklad způsobu výsledného vyjádření dopadu s využitím součtu hodnot jednotlivých kritérií*:***

| *Součet K1–K4* | *Úroveň dopadu* | *Význam* |
|---|---|---|
| *4–7* | *Nízký* | *Omezené dopady, lokální charakter* |
| *8–11* | *Střední* | *Zvládnutelné, ale významné dopady* |
| *12–15* | *Vysoký* | *Závažné dopady na klíčové oblasti* |
| *16–20* | *Kritický* | *Zásadní dopady na fungování / regulované služby* |

### Důraz na konzistenci a obhajitelnost

Při stanovení výsledné úrovně dopadu je důležitější konzistentní přístup než samotná volba konkrétní škály nebo způsobu agregace. Organizace by měla používat stejný přístup napříč hodnocenými riziky správy dat a být schopna vysvětlit, jakým způsobem k výsledné úrovni dopadu dospěla.

Výsledná úroveň dopadu by měla být vždy:

- srozumitelná pro vlastníky dat a vedení organizace,
- porovnatelná napříč různými riziky správy dat,
- využitelná jako vstup pro stanovení priority rizika a plánování opatření.

## 4.5 Vztah úrovně dopadu k prioritě rizika

Stanovení priority rizika správy dat navazuje na výslednou úroveň dopadu určenou v předchozí kapitole. Priorita vyjadřuje relativní význam rizika z hlediska potřeby jeho dalšího řešení, nikoli absolutní míru jeho závažnosti. Slouží jako praktický nástroj pro rozhodování o tom, kterým rizikům má být věnována pozornost přednostně a v jakém rozsahu.

Pro účely tohoto návodu se doporučuje vycházet **z jednoduchého převodu výsledné úrovně dopadu na prioritu rizika**, například rozlišením nízké, střední, vysoké a kritické priority. Konkrétní prahové hodnoty, označení úrovní nebo jejich počet nejsou tímto dokumentem předepsány a mohou být přizpůsobeny potřebám organizace.

Priorita rizika správy dat by měla být vždy stanovena v kontextu organizace, zejména s ohledem na:

- význam dotčených dat pro plnění agend a rozhodování,
- existující opatření a schopnost organizace riziko zvládat,
- kapacity dostupné pro řízení rizik a realizaci opatření.

Stanovení priority rizika neznamená automaticky povinnost okamžité realizace opatření. Priorita slouží především k:

- uspořádání rizik podle jejich významu,
- podpoře plánování opatření v oblasti správy dat,
- transparentní komunikaci rizik směrem k vedení organizace.

Priorita rizika správy dat je relativní a může se v čase měnit v závislosti na změnách v organizaci, jejích datech, agendách nebo vnějších podmínkách. Z tohoto důvodu je vhodné priority rizik pravidelně přezkoumávat, zejména při významných změnách nebo v rámci pravidelných přezkumů řízení rizik.

## 4.6 Použití výsledků hodnocení a návaznost na řízení rizik kybernetické bezpečnosti

Výsledky hodnocení dopadu a stanovení priority rizik správy dat slouží primárně jako podklad pro řízení rizik v oblasti správy dat, zejména pro plánování a realizaci preventivních a nápravných opatření. V některých případech však mohou mít rizika správy dat významné dopady i z pohledu kybernetické bezpečnosti, a to zejména tehdy, pokud se dotýkají regulovaných služeb, klíčových aktiv nebo bezpečnostních cílů organizace.

### Eskalace rizik správy dat do řízení rizik kybernetické bezpečnosti

Rozhodnutí o eskalaci rizika správy dat do řízení rizik kybernetické bezpečnosti se opírá o význam dopadů rizika, nikoli výhradně o existenci přímého mapování zranitelností nebo hrozeb na typové zranitelnosti či typové hrozby podle rámce NÚKIB. Eskalace může být opodstatněná i v situacích, kdy takové mapování neexistuje, pokud dopady rizika správy dat představují z pohledu organizace relevantní hrozbu pro kybernetickou bezpečnost.

Katalog rizik správy dat obsahuje rovněž mapování situací, ve kterých mohou již samotné dopady rizik správy dat (bez jejich prioritizace v kontextu konkrétní organizace) představovat hrozbu v oblasti kybernetické bezpečnosti. Tato mapování slouží jako podpůrný analytický nástroj pro identifikaci případů, kdy je vhodné riziko správy dat posoudit také v kontextu kybernetické bezpečnosti, a to i bez přímé vazby na typové hrozby nebo zranitelnosti NÚKIB (více informací je uvedeno v „Návodu pro práci s Excel katalogem“).

### Role primárních a sekundárních dopadů při eskalaci

Při posuzování návaznosti na řízení rizik kybernetické bezpečnosti vychází stanovení priority rizika správy dat nadále z hodnocení jeho primárního dopadu. Zároveň však mohou sekundární dopady poskytnout důležité informace o širším bezpečnostním kontextu rizika.

Sekundární dopady mohou zejména:

- upozornit na vazby rizika správy dat na regulované služby nebo klíčová aktiva,
- signalizovat možné ohrožení důvěrnosti, integrity nebo dostupnosti informací,
- podpořit rozhodnutí o eskalaci rizika do řízení rizik kybernetické bezpečnosti.

Sekundární dopady však nemění stanovenou prioritu rizika správy dat a nejsou samostatně hodnoceny z hlediska úrovně dopadu. Slouží jako kontextový prvek, který doplňuje pohled na riziko při rozhodování o jeho dalším řešení.

### Vymezení odpovědností a návaznost procesů

Eskalace rizika správy dat do řízení rizik kybernetické bezpečnosti neznamená převzetí odpovědnosti za řízení rizika kybernetickou bezpečností. Riziko správy dat zůstává i nadále řízeno v rámci správy dat, zatímco řízení rizik kybernetické bezpečnosti posuzuje relevantní dopady z hlediska bezpečnostních cílů a regulačních požadavků.

Tento přístup umožňuje koordinované a komplementární řízení rizik, kdy jsou využívány existující procesy kybernetické bezpečnosti, aniž by byla oslabena role správy dat nebo narušena konzistence metodického rámce.

## 4.7 Možnost alternativních přístupů k hodnocení dopadu

Tento návod popisuje doporučený referenční postup hodnocení dopadu rizik správy dat, který je navržen tak, aby byl použitelný v širokém spektru organizací veřejné správy. Organizace však mohou využít i jiný způsob hodnocení dopadu, pokud je tento způsob v souladu s principy stanovenými „Metodikou řízení rizik správy dat“.

Alternativní přístup k hodnocení dopadu rizik správy dat by měl zejména:

- vycházet z posouzení dopadů rizik správy dat, nikoli z pravděpodobnosti jejich výskytu,
- reflektovat význam dat pro agendy, rozhodování a fungování organizace,
- vést k určení srozumitelné a obhajitelné úrovně dopadu a priority rizika.

Bez ohledu na zvolený přístup by výsledky hodnocení dopadu měly být srovnatelné svým významem a využitelností. Organizace by měla být schopna vysvětlit, jakým způsobem k výsledné úrovni dopadu dospěla, a doložit, že zvolený postup je aplikován konzistentně napříč hodnocenými riziky správy dat.

Při využití alternativního přístupu se doporučuje tento přístup stručně popsat a zdokumentovat, aby byla zajištěna transparentnost a možnost návaznosti na další procesy, zejména na řízení rizik kybernetické bezpečnosti.

## 4.8 Referenční postup hodnocení dopadu a priority rizika správy dat (doporučený postup)

Tato část popisuje doporučený referenční postup, jak v praxi provést hodnocení dopadu a stanovení priority rizika správy dat. Postup vychází z principů uvedených v „Metodice řízení rizik správy dat“ a zohledňuje vazby na řízení rizik kybernetické bezpečnosti. Organizace mohou tento postup převzít v plném rozsahu nebo jej přizpůsobit svému kontextu v souladu s kapitolou 4.7.

### Krok 1 – Určení dopadů rizika (typové dopady TD1–TD14)

1. Pro hodnocené riziko správy dat identifikujte možné dopady s využitím typových dopadů katalogu rizik správy dat (TD1–TD14).
2. Z identifikovaných dopadů určete:
    - jeden primární dopad, který nejlépe vystihuje hlavní škodu způsobenou realizací rizika,
    - případně jeden nebo více sekundárních dopadů, které popisují další relevantní následky.
3. Primární dopad bude dále použit pro hodnocení dopadu a stanovení priority rizika. Sekundární dopady slouží jako kontextová informace a pro posouzení návazností (např. eskalace do kybernetické bezpečnosti).

## Krok 2 – Hodnocení primárního dopadu pomocí kritérií K1–K4

Primární dopad rizika se posoudí z následujících čtyř hledisek:

**K1 – Rozsah dopadu**

- Kolik agend, procesů nebo datových oblastí je dopadem zasaženo?
- Jedná se o lokální nebo plošný dopad?

**K2 – Intenzita dopadu**

- Jak závažně je ovlivněno fungování organizace nebo kvalita rozhodování?
- Dochází k zásadnímu omezení klíčových činností?

**K3 – Náklady a úsilí na nápravu**

- Jak náročná je náprava dopadů (časově, organizačně, finančně)?
- Vyžaduje zapojení více útvarů nebo externích subjektů?

**K4 – Reputační, právní a strategický dopad**

- Může dojít k poškození důvěry, právním důsledkům nebo ohrožení strategických cílů?

**Každému kritériu se přiřadí hodnota na škále 1–5, kde:**

- 1 = zanedbatelný dopad,
- 5 = velmi závažný dopad.

## Krok 3 – Výpočet výsledného dopadu

Hodnoty přiřazené jednotlivým kritériím K1–K4 se **sečtou**. Na základě dosaženého součtu se stanoví **výsledná úroveň dopadu** podle čtyř úrovňové škály, která je významově kompatibilní s rámcem řízení rizik kybernetické bezpečnosti.

**Doporučený převod:**

| Součet K1–K4 | Úroveň dopadu | Význam |
|---|---|---|
| 4–7 | Nízký | Omezené dopady, lokální charakter |
| 8–11 | Střední | Zvládnutelné, ale významné dopady |
| 12–15 | Vysoký | Závažné dopady na klíčové oblasti |
| 16–20 | Kritický | Zásadní dopady na fungování / regulované služby |

Výsledná úroveň dopadu představuje **rozhodovací kategorii**, nikoli exaktní kvantifikaci závažnosti rizika.

## Krok 4 – Stanovení priority rizika

Výsledná úroveň dopadu se přímo promítá do priority rizika správy dat:

- Kritický dopad → kritická priorita
- Vysoký dopad → vysoká priorita
- Střední dopad → střední priorita
- Nízký dopad → nízká priorita

Tento převod zajišťuje, že výsledky prioritizace rizik správy dat jsou přímo čitelné a použitelné v rámci řízení rizik kybernetické bezpečnosti.

### Krok 5 – Posouzení eskalace do řízení rizik kybernetické bezpečnosti

Na základě:

- výsledné priority,
- charakteru primárního i sekundárních dopadů,
- a kontextu regulovaných služeb nebo klíčových aktiv,

se posoudí, zda má být riziko správy dat eskalováno do řízení rizik kybernetické bezpečnosti.

Eskalaci lze provést:

- i bez přímého mapování na typové hrozby nebo zranitelnosti NÚKIB, pokud dopady rizika představují relevantní hrozbu z pohledu kybernetické bezpečnosti.

Do řízení rizik kybernetické bezpečnosti se eskaluje výsledek prioritizace a popis dopadů, nikoli samotný proces hodnocení rizika správy dat.

## 4.9 Typické chyby a doporučení

Při hodnocení dopadu rizik správy dat může dojít k následujícím typickým chybám, které mohou vést ke zkreslení výsledků prioritizace nebo ke snížení jejich využitelnosti.

### Zaměňování dopadu a pravděpodobnosti

Jednou z nejčastějších chyb je posuzování rizika správy dat podle pravděpodobnosti jeho výskytu namísto podle dopadu. Tento přístup je v rozporu s principy metodiky a může vést k podcenění rizik, která mají nízkou pravděpodobnost, ale vysoký dopad na fungování organizace.

### Snaha o nadměrnou kvantifikaci

Pokusy o příliš detailní nebo exaktní kvantifikaci dopadů mohou vytvářet falešný dojem přesnosti a zbytečně zatěžovat proces hodnocení. Hodnocení dopadu má sloužit jako podklad pro rozhodování, nikoli jako matematický model. Důležitější, než přesná čísla je konzistentní a obhajitelný přístup.

### Opomíjení významu dat a kontextu organizace

Hodnocení dopadu bez znalosti významu dotčených dat, jejich role v agendách a vazeb na rozhodování organizace může vést k nepřesným závěrům. Posouzení dopadu by mělo vždy vycházet z konkrétního organizačního kontextu a zapojovat role, které mají k datům věcný vztah.

### Nejasné určení primárního dopadu

Nedostatečně vymezený nebo nejednoznačně určený primární dopad ztěžuje následné hodnocení a oslabuje srozumitelnost výsledků. Před zahájením hodnocení dopadu je proto vhodné věnovat pozornost jasnému určení, v čem spočívá hlavní význam rizika správy dat.

### Ignorování sekundárních dopadů

Ačkoli sekundární dopady nejsou zahrnovány do výpočtu úrovně dopadu, jejich úplné opomenutí může vést k přehlédnutí důležitých souvislostí, zejména vazeb na regulované služby nebo kybernetickou

bezpečnost. Sekundární dopady by měly být zaznamenány a využity při návrhu opatření a posouzení návazností.

## Nedostatečná dokumentace a nekonzistentní přístup

Hodnocení dopadu prováděné bez základní dokumentace nebo s různými přístupy u jednotlivých rizik snižuje jeho obhajitelnost a využitelnost. I při zjednodušeném postupu je důležité zachovat konzistenci a být schopen vysvětlit, jakým způsobem byly jednotlivé závěry dosaženy.